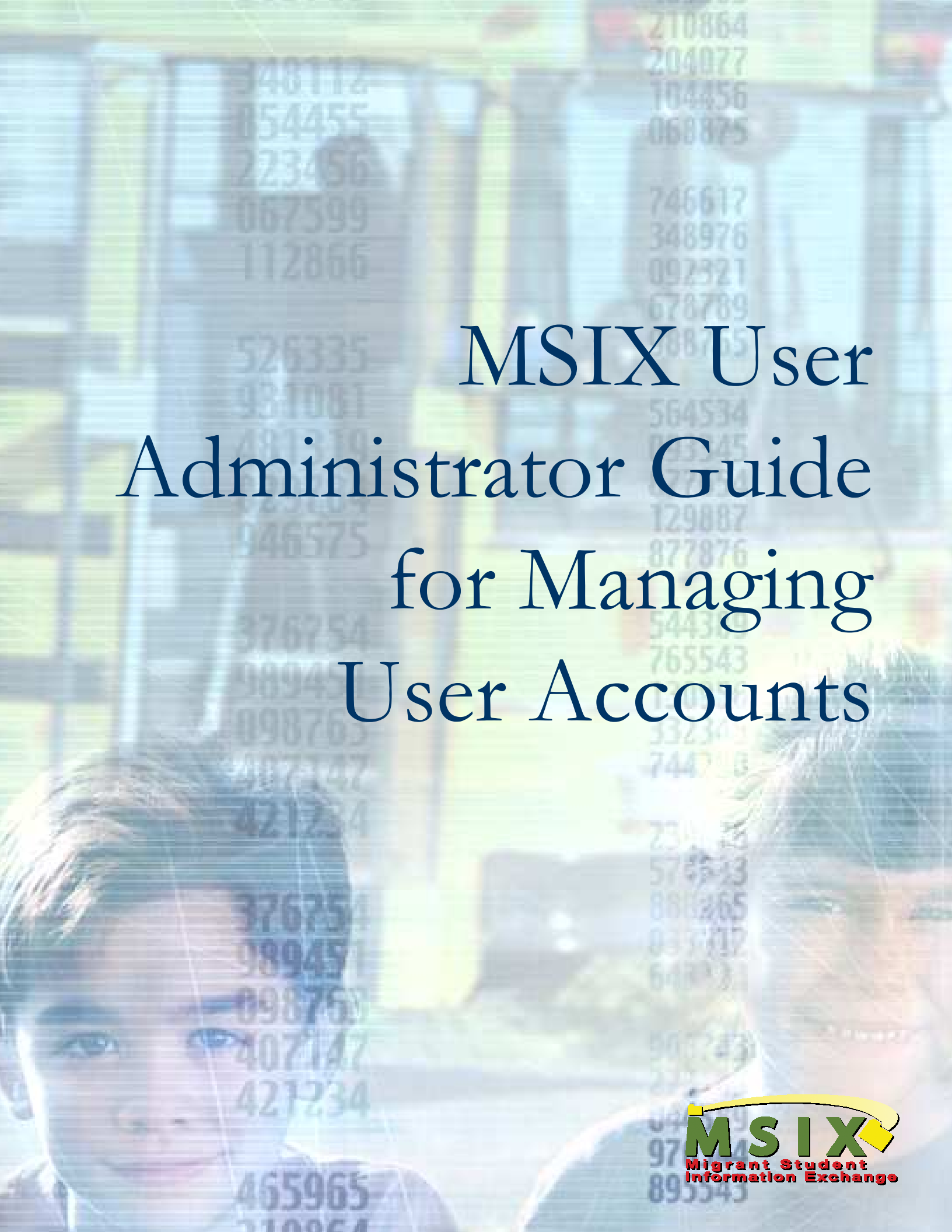

MSIX User Administrator Guide for Managing User Accounts

MSIX
Migrant Student Information Exchange

U.S. DEPARTMENT OF EDUCATION

MSIX User Administrator Guide for Managing User Accounts

June 2008

"MSIX IS AVAILABLE TO AUTHORIZED USERS ONLY"

Table of Contents

User Management Overview

Purpose

This *MSIX User Administrator Guide for Managing User Accounts* outlines the process that MSIX User Administrators must follow when administering accounts for authorized users of the Migrant Student Information Exchange (MSIX) application. This guide covers the various phases of the User Management Lifecycle including the Request, Provide, Review, and Revoke steps. It also serves as a supplement to the Rules of Behavior that define the acceptable behavior expected of MSIX users.

This guide lays out policies and procedures for accessing MSIX to help user administrators understand the User Management Lifecycle as it pertains to MSIX. It also documents guidelines for the user administrators. Additional information is available to user administrators via the training materials and user guides available within MSIX.

Background

The No Child Left Behind Act (NCLB) of 2001 mandated that the U.S. Department of Education (ED) ensures that all students have equal access to education and that ED promotes educational excellence throughout the nation. The Office of Migrant Education (OME), part of ED's Office of Elementary and Secondary Education (OESE), is responsible for administering the Migrant Education Program (MEP). The MEP supports State Educational Agencies (SEAs) by providing funding to help SEAs establish or improve educational programs for migrant students.

Section 1308(b) of the NCLB requires the OME to assist States in developing effective methods for electronically exchanging student records amongst States and to determine an accurate count of the number of migratory children in each State. OME established the MSIX initiative to satisfy these requirements and support their goals for the MEP through MSIX.

Welcome to MSIX

The MSIX homepage (see Figure 1) is the initial page that appears after a successful login and the Rules of Behavior (ROB) have been accepted. The ROB is included in this document as Appendix A.

Before using MSIX, all computers will need to meet the following system requirements:

- Access to the internet using Internet Explorer v5.5 or higher, Firefox v1.5 or higher, Netscape v7.0 or higher, or Safari v2.0 or higher
- Adobe Flash Player (version 6 or later) must be installed in order to view the online training content. Adobe Flash Player is often part of the standard software provided with most computers. The player can also be downloaded from www.adobe.com. Users without access to Adobe Flash Player should refer to the MSIX User Manual for guidance and information about using MSIX.

Figure 1 – MSIX Homepage

Roles and Responsibilities

User Management Lifecycle Roles

The following key players are involved in the User Management Lifecycle:

- **Applicant** — the individual applying for an MSIX user account
- **Verifying Authority** — a trusted individual that verifies the identity of a subscriber for the user administrators
- **User Administrator** — a trusted individual that creates user login credentials (i.e., user id and password) and maintains users within MSIX. Their tasks include creating, modifying, and deactivating user accounts.

MSIX User Roles

The following table describes the user roles that have been defined within MSIX. It also includes a description of the user's responsibilities, functions within the system, and potential users.

MSIX User Roles and Responsibilities			
User Role	**Description**	**Functions Allowed**	**Potential Users**
School and District Level Roles			
MSIX Primary	MSIX Primary Users can query student records in all states. This user can also initiate the merge and split process for student records in his or her state.	▪ Search, display, and print student records for students in all states ▪ Initiate merge and split of student records ▪ Email notification of an arrival or departure of a student ▪ Export Student Records to File	▪ Guidance Counselors ▪ MEP Data Entry Staff ▪ Recruiters ▪ Registrars ▪ Teachers
MSIX Secondary	MSIX Secondary Users can query student records in all states.	▪ Search, display, and print student records for students in all states ▪ Email notification of an arrival or departure of a student	▪ Guidance Counselors ▪ MEP Data Entry Staff ▪ Recruiters ▪ Registrars ▪ Teachers
District Data Administrator	District Data Administrators can validate or reject near matches, merges and splits of student records. This user can also initiate the merge and split process for student records in his or her district.	▪ Search, display, and print student records for students in all states ▪ Generate Reports ▪ Initiate merge and split of student records ▪ Validate or reject record near matches, merges and splits ▪ Resolve data quality issues ▪ Respond to escalation requests ▪ Email notification of an arrival or departure of a student ▪ Export Student Records to File	▪ State MEP Administrators ▪ MEP Data Entry Staff
Regional Level Roles			
Regional Data Administrator	Regional Data Administrators can validate or reject near matches, merges and splits of student records. This user can initiate the merge and split process for student records in his or her region. This user will also serve as the secondary point of contact for escalation issues.	▪ Search, display, and print student records for students in all states ▪ Generate Reports ▪ Initiate merge and split of student records ▪ Validate or reject record near matches, merges and splits ▪ Resolve data quality issues ▪ Respond to escalation requests ▪ Email notification of an arrival or departure of a student ▪ Export Student Records to File	▪ State MEP Administrators ▪ MEP Data Entry Staff
Regional User Administrator	Regional User Administrators establish and manage user accounts for users in their region.	▪ Create User accounts ▪ Assign User Role(s) ▪ Update User account information ▪ Deactivate User accounts ▪ Reset passwords	▪ State-identified
State Level Roles			
State Data Administrator	State Data Administrators can validate or reject near matches, merges and splits of student records. This user can initiate the merge and split process for student records in their state. He or she can also resolve data quality issues and serve as the primary point of contact for escalation issues.	▪ Search, display, and print student records for students in all states ▪ Generate Reports ▪ Initiate merge and split of student records ▪ Validate or reject record near matches, merges and splits ▪ Resolve data quality issues ▪ Respond to escalation requests ▪ Email notification of an arrival or departure of a student ▪ Export Student Records to File	▪ State MEP Administrators ▪ MEP Data entry staff
State User	State User Administrators establish and manage user	▪ Create User accounts ▪ Assign User Role(s)	▪ State-identified

MSIX User Roles and Responsibilities			
User Role	**Description**	**Functions Allowed**	**Potential Users**
Administrator	accounts for users in their state.	▪ Update User account information ▪ Deactivate User accounts ▪ Reset passwords	
State Region Administrator	State Region Administrator establishes and maintains the regional structure and associated districts for states that choose to use regions.	▪ Enable and disable regional structure ▪ Create new regions ▪ Associate districts to regions ▪ Edit regions	▪ State MEP Administrators ▪ MEP Data entry staff
U.S. Department of Education (ED) User Roles			
Government Administrator	Government Administrators can generate summary level standard and ad hoc queries on a State, Regional, or National level.	▪ Generate Reports	▪ OME
OME User Administrator	OME User Administrators establish and manage user accounts for all State User Administrators.	▪ Create user accounts ▪ Assign State User Administrator role ▪ Update user account information ▪ Deactivate user accounts ▪ Reset passwords	▪ OME
Privacy Act Administrator	Privacy Act Administrators can enter statements provided by students and parents that formally dispute the data contained in a student's MSIX record. They can also query and view student records from all states.	▪ Search, display, and print student records ▪ Enter dispute statements into a student's MSIX record	▪ OME

Table 1 – MSIX User Roles and Responsibilities

Account Status

The status of a user's account may be Pending, Active (Enabled), Disabled, or Deactivated. This user account status is explained in further detail in the following table:

MSIX User Account Status		
Status	**Description**	**Example**
Pending	The Pending status applies to user accounts that a user administrator has created in MSIX, but, are not active until they reach the specified account activation date.	A State User Administrator creates a new primary user account in July for Jane Doe. Jane is scheduled to start her new job as a guidance counselor in September. Her account's activation date is set to coincide with her start date. Jane's account is in "Pending" status until the activation date.
Active (Enabled)	The Active status applies to user accounts that are fully operational and have been set to "Enabled" by a user administrator.	Jane begins work in September. Her primary user account is active and she is able to successfully login into MSIX.

MSIX User Account Status		
Status	**Description**	**Example**
Disabled	The "Disabled" status applies to a user account that is temporarily not accessible by the user. MSIX accounts can become disabled for several reasons such as: ▪ **Incorrect Login Lockout** – After 3 consecutive invalid login attempts, MSIX accounts are automatically disabled. ▪ **Expired Accounts** – User accounts are disabled when they reach the expiration date specified on the User Administration page. ▪ **Inactive Accounts** – User accounts are automatically disabled after 90 days of inactivity. ▪ **Manually Disabled** – User administrators may manually disable an account by selecting the Disable Account button on the Update User page.	Jane has a difficult time remembering her password. After she tries 3 times to login without success, her account is automatically disabled.
Deactivated	The "Deactivated" status applies to user accounts that a user administrator has manually deactivated in MSIX through the User Administration window. These accounts are permanently closed and cannot be reactivated.	After several years as a guidance counselor, Jane resigns from her job to pursue another job opportunity. The Texas user administrator deactivates her account since Jane will no longer need access to MSIX.

Table 2 – MSIX User Account Status

User Management Lifecycle

The User Management Lifecycle includes four phases to Request, Provide, Review, and Revoke user access.

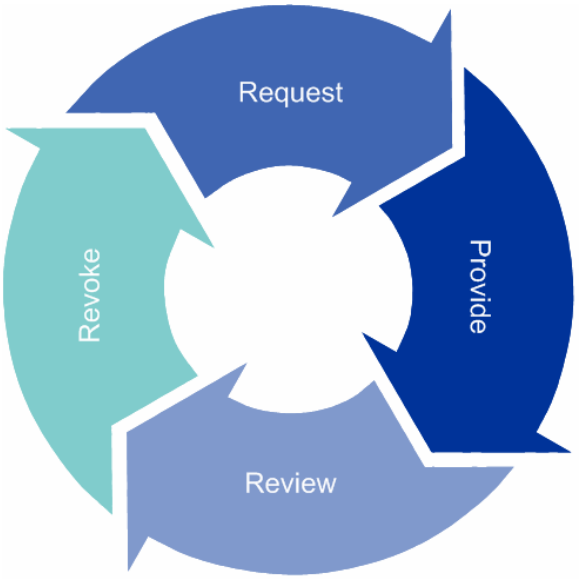

Figure 2 – MSIX User Management Lifecycle

To obtain access to MSIX, users will go through the Request and Provide phases. Each phase contains multiple steps that must be completed to successfully obtain access to MSIX. Figure 3 below and the following sections provide further insight into these phases.

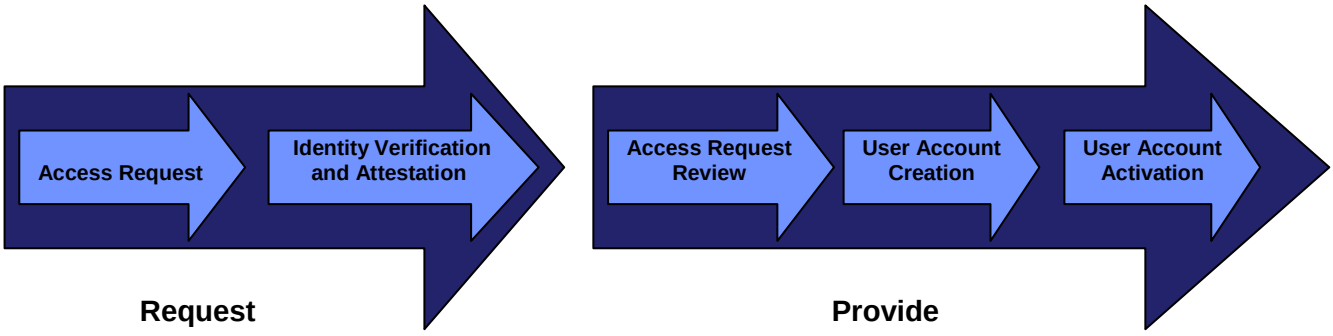

Figure 3 – Request and Provide Phases

Request

The Request phase is composed of the following steps:

- **Access Request** — The applicant applies for access to MSIX.
- **Identity Verification and Attestation** — The Verifying Authority reviews and verifies the applicant's identity and information on the *User Application for Access to MSIX* form.

Access Request

An application, *User Application for Access to MSIX,* for a user account to MSIX can be obtained through the MSIX login screen (http://msix.ed.gov) by clicking the How Do I Get an Account? link. No login is required. This form is a guideline created to help states with the user registration process. If this form is used, it must be completed in its entirety. Only portions of the form are shown in this guide; the full version should be obtained on the MSIX website.

Applicant Information

- Complete the applicant information below and sign the form.
- Forward the form to a Verifying Authority. This should be your direct supervisor or an individual that is above the direct supervisor in an official reporting structure. Provide appropriate identification information.

First Name		Last Name			
Title					
Work Address	*Street*	*City*		*State*	*Zip*
Work Email		Work Telephone	*XXX-XXX-XXXX* – – Ext.		
Region (if applicable)		School District (if applicable)			

MSIX Account Information

MSIX Role(s)	☐ MSIX Primary User ☐ MSIX Secondary User	☐ Regional User Administrator ☐ State User Administrator	☐ District Data Administrator ☐ Regional Data Administrator ☐ State Data Administrator	☐ State Region Administrator

Signature

I certify that this information is accurate and complete to the best of my knowledge. I will only use MSIX in accordance with the MSIX Rules of Behavior.

Signature: _____ Date: _____

The Privacy Act of 1974 (5 U.S.C. § 552a)

Figure 4 – Applicant Information Section, *User Application for Access to MSIX* Form

Applicant Information

- **First Name** and **Last Name** — the legal name of the individual requesting access to MSIX
- **Title** — the applicant's job title or description such as Teacher, Guidance Counselor, or Student Registrar
- **Work Address** — the street, city, state and zip code of applicant's workplace
- **Work Email** — the applicant's workplace email address
- **Work Telephone** — the applicant's workplace telephone number

The address, email, and telephone number provided on the application may be used to contact the applicant about MSIX matters.

MSIX Account Information

- **Region** and **District** — the region and district where the applicant works
  Both fields are optional for roles that are not region or district specific; not all states have a regional structure.
- **MSIX Role** — the desired MSIX user role(s) — see Table 1, *"MSIX User Roles and Responsibilities."*

Signature

- **Signature** — the applicant's certification that the information provided is accurate and complete
- **Date** — the date the applicant signed the application

Once an MSIX user account has been created, the user can update their phone number and password using the **My Account** page in MSIX. Users will need to contact a User Administrator to make any other changes to their account, such as changes to their name, work address, or email address.

Identity Verification and Attestation

Identity Verification and Attestation is the second step in the Request phase. The identity of MSIX applicants should be confirmed by a Verifying Authority. The applicant's direct supervisor or an individual that is above the direct supervisor in an official reporting structure should perform the identity verification. For example, an applicant who is a teacher should submit the application to his/her principal for identity verification review, or an applicant who is a state MEP administrator should submit to his/her MEP Director for identity verification.

When approving a user's access request form, the user's identity should be verified (e.g., reviewing their State/District issued ID badge, driver's license, passport, etc.). As approver of system access, the Verifying Authority is responsible for verifying the applicant's identity. The person responsible for approving access for an identified resource can be held accountable for the actions of that user. The Verifying Authority must review each field of the application for accuracy and completeness. The Verifying Authority will also verify that the applicant's MSIX role(s) is appropriate for the applicant's job.

Upon successful verification of identity, the Verifying Authority will complete and sign the Identity Verification and Attestation portion of the application (see Figure 5) and retain a copy of the application in the local records.

Identity Verification and Attestation

- As the Verifying Authority, you should be the Applicant's direct supervisor or an individual that is above the direct supervisor in an official reporting structure.
- Review the entire application for completeness and accuracy.
- Complete the information below, confirm the Applicant's identification, attest to his/her need of an MSIX account, and confirm that the Applicant has the right level of access.
- Upon completion, file the form in your local records and return this form to the Applicant.

Verifying Authority First Name		Verifying Authority Last Name	
Title			
Work Email		Work Telephone	*XXX-XXX-XXXX* – – Ext.
Organization		Applicant Identity Verification Method	☐ State Driver's License ☐ State / District ID ☐ Passport ☐ Other: _____
Account Effective Date (optional)		Account End Date (optional)	

Signature

I certify that: 1) I have verified the identity of the above applicant; 2) I have determined that he or she has a need for MSIX information; and 3) the above-mentioned individual is requesting the appropriate MSIX role(s).

Signature: _____ Date: _____

The Privacy Act of 1974 (5 U.S.C. § 552a)

Figure 5 – Identity Verification and Attestation Section, *User Application for Access to MSIX* Form

Identity Verification and Attestation

- **Verifying Authority First Name** and **Verifying Authority Last Name** — the legal name of the Verifying Authority reviewing the application
- **Title** — the official title or position of the Verifying Authority
- **Work Email** — the Verifying Authority's work email address
- **Work Telephone** — the Verifying Authority's workplace telephone number

  The phone number may be used if the Verifying Authority needs to be contacted about MSIX matters.
- **Organization** — the organization or entity that employs the Verifying Authority
- **Applicant Identity Verification Method** — the type of ID or method used to verify the identity of the applicant
- **Account Effective Date** and **Account End Date** — optional fields that can be used to designate a known future start or end date for a user account

  For instance, a future Account End Date may be entered for a seasonal employee that will no longer need access to MSIX after the summer months.

Signature

- **Signature** — the Verifying Authority's certification that the information provided is accurate and complete

- **Date** — the date the applicant signed the application

Provide

The Provide phase is the second part in the process to obtain access to MSIX. It is composed of the following steps:

- **Access Request Review** — User Administrator's review of the application to verify that all of the required information has been provided
- **User Account Creation** — when the User Administrator creates the User's account
- **User Account Activation** — when the User account is activated

Access Request Review

Each state may have State User Administrators, Regional User Administrators, or both. The User Administrator will create an account in MSIX for the applicant requesting access based on information provided in the application. The application should be delivered to the User Administrator's office.

Users will find the name and contact information for their state or regional User Administrator by clicking on the **How Do I Get an Account?** link from the MSIX home page (msix.ed.gov) or by contacting their state's Migrant Education Program office.

The User Administrator will review the applications received to verify that both the Applicant and Verifying Authority sections are complete. After this, the User Administrator will complete his/her own information (see Figure 6), sign the form, and file it in his/her local records. If any problems are identified during the review, the User Administrator will contact the Applicant and/or the Verifying Authority that reviewed the application.

State/Regional Authority Approval

- Review the Applicant and Verifying Authority portions of the application for completeness.
- Complete the information below, sign, and file the form in your local records.
- Create an MSIX account for the Applicant.

Approving Authority First Name		Approving Authority Last Name			
Title		Role	☐ Regional User Administrator ☐ State User Administrator		
Work Address	*Street*	*City*		*State*	*Zip*
Work Email		Work Telephone	*XXX-XXX-XXXX* – – Ext.		

Signature

I certify that this information is accurate and complete to the best of my knowledge and I hereby grant to the above-mentioned individual the MSIX role for which they have applied.

Signature: _____ Date: _____

The Privacy Act of 1974 (5 U.S.C. § 552a)

Figure 6 – State/Regional Authority Approval Section, *User Application for Access to MSIX* Form

State/Regional Authority Approval

- **Approving Authority First Name** and **Approving Authority Last Name** — the legal name of the Approving Authority reviewing the application
- **Title** — the official title or position of the Approving Authority
- **Role** — the position of the Approving Authority representing either the regional or state level
- **Work Address** — the street, city, state and zip code of Approving Authority's workplace
- **Work Email** — the Approving Authority's work email address
- **Work Telephone** — the Approving Authority's workplace telephone number

  The phone number may be used if the Approving Authority needs to be contacted about MSIX matters.

Signature

- **Signature** — the Approving Authority's certification that the information provided is accurate and complete
- **Date** — the date the applicant signed the application

Upon successfully completing the review, the user administrator will create accounts for the applicants requesting access to MSIX based upon the information provided in their application.

User Account Creation

Once the user administrator successfully reviews the application, he/she can create a new user account using the following steps:

Steps to Create User Account

1. Click the **User Administration** link on the left navigation.
2. Click the **Create New User** link in the main body section of the User Administration page.
3. On the Create New User page, enter at a minimum all required information to create a new user, including the **First Name**, **Last Name**, **Telephone Number**, **Email Address**, **Location** (State), and **User Role.**
4. Click the **Next** button.
5. Verify that the User Information displayed on the Confirmation page is correct.

   For roles such as District Data Administrator, Regional Data Administrator, or Regional User Administrator, select the applicable **Region** or **District** information from the lists provided.
6. Click the **Save** button.

Once the user account information has been successfully entered into MSIX, the User Administrator will be taken to a Confirmation page that indicates that the new account was successfully created. MSIX will generate an email notification to the new user, using the email

address entered by the User Administrator, to notify the new user of his/her new MSIX Username and provide information about accessing MSIX.

The User Administrator will be copied on this message as an additional confirmation that the account was created and the new user notified. MSIX will generate a second separate email message to the new user only, containing the initial password for his/her new MSIX account. The new MSIX user will be required to reset this password when he/she first accesses MSIX.

Username and Password Specifications

MSIX has the following specifications for the username and password:

- **Username** — MSIX will automatically generate each username.
- **Password** — Minimum password length and special characteristics are used when MSIX automatically generates each user's initial password. Any new password created by the user must be at least eight characters, contain at least one upper case letter (A-Z), at least one lower case letter (a-z), at least one number (1-9), and a special character (e.g., !, @, #, $), all with no spaces in between.

User Account Activation

MSIX will activate the user's account on the date specified by the User Administrator in the Account Activation Date field. If that is a future date, MSIX will keep the user account in pending status until it reaches that date. If no activation date is specified, the account will be activated immediately.

When the user logs into MSIX for the first time, he/she is prompted to perform the following actions:

- **Review MSIX Training Materials** — The Training Materials must be reviewed by each user before proceeding to the Rules of Behavior. They can also be reviewed at any time by clicking on the Training link at the top of any MSIX page.
- **Accept the Rules of Behavior (ROB)** — MSIX will present the user with the ROB and be asked to either accept or decline them. If the user does not accept the ROB, the user is unable to successfully login to MSIX and MSIX will redirect the user to the Login screen. MSIX will require each user to accept the ROB before granting him/her access.
- **Change Password** — MSIX will prompt users to change their password upon their first successful login. MSIX will direct the user to his/her homepage and will display a greeting message upon a successful login.

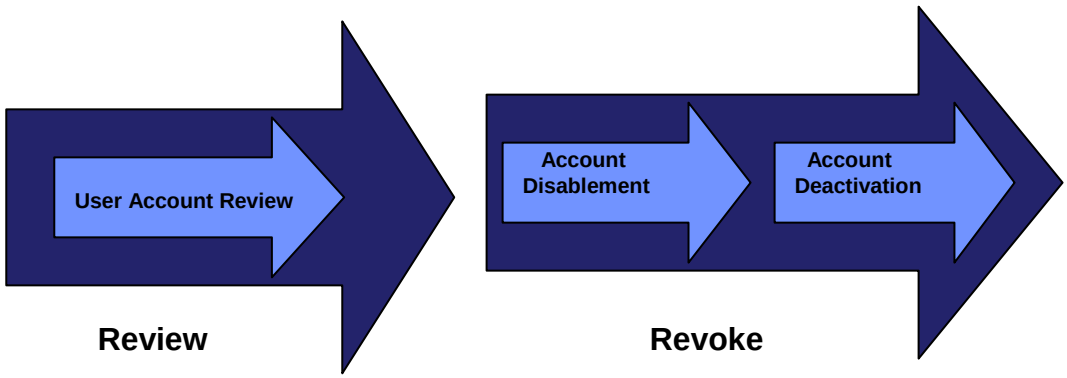

Figure 7 – Review and Revoke Phases

Review

The Review phase involves reviewing the user accounts for auditing and compliance purposes.

User Account Review

The User Account Review is the step that the User Administrator performs to build a high quality accountability system. An Annual Security Compliance Review is an assessment to determine if the individual MSIX users have the appropriate level of access to MSIX. It is a best practice for user administrators to complete the Security Compliance Review on an annual basis. However, ED encourages user administrators to complete the compliance review on a more frequent basis.

The User Administration page in MSIX provides key dates to assist in the annual review of user accounts. At the bottom of the page, the following dates are provided for each user account:

- **Account Creation Date** — the date the user account was initially created
- **First Login Date** — the date the user first accessed this account
- **Last Login Date** — the date the user most recently accessed this account – Use the User Account List Report to create a list of all user accounts with the date they last accessed MSIX.
- **Account Deactivation Date** — the date the account was permanently deactivated (this will be blank for active and disabled accounts)
- **ROB Acceptance Date** — the date the user accepted the MSIX Rules of Behavior

User Administrators can review the information provided in these fields to verify the user is still actively using MSIX. The Last Login Date will indicate how recently MSIX was used. Secondly, dates should be displayed in the ROB Acceptance Date field to confirm compliance of this activity.

Revoke

The Revoke phase is one of the most important parts in preventing unauthorized access to MSIX. Employees and supervisors must immediately notify their MSIX user administrator when access to MSIX is no longer required. This is a manual process, and if not followed carefully, can result in security risk and exposure.

User administrators can disable and deactivate user accounts. The user administrators are responsible for revoking an MSIX user's access if the user is no longer part of the organization or if the user no longer requires access to MSIX.

Account Disablement

User accounts can be manually disabled by user administrators or automatically by MSIX. This is a **temporary change**. A user administrator can later reactivate a disabled account. Note, the Help Desk does not reset passwords, create new users, deactivate, or disable existing users.

Disable Manually

If a user administrator is notified that a user's role has changed or no longer needs access to MSIX, they can disable the user account immediately. The user administrator can also set a future date to disable a user. MSIX will then automatically disable the user account on the specified date. To disable user accounts manually, the following steps should be followed:

Steps to Disable User Account

1. Click the **User Administration** link on the left navigation.

2. On the Create New User page, change the **Account Status** to **Disabled**.
3. Click the **Save** button.

Steps to Disable User Account For a Future Date

1. Click the **User Administration** link on the left navigation.
2. On the Create New User page, change the **Account Expiration Date** to a future date.
3. Click the **Save** button.

Disable Automatically

MSIX has built in functionality that will disable user accounts automatically in certain situations. These situations include:

- **Login / Lock Out** — Incorrect login lockout is after 3 consecutive invalid login attempts, MSIX accounts are automatically disabled.
- **Expired Accounts** — Expired accounts are user accounts that are disabled when the account reaches the expiration date specified on the User Administration page.
- **Inactive Accounts** — Inactive accounts are user accounts are automatically disabled after 90 days of inactivity.

Reactivate Disabled Accounts

If a user account has been disabled, the user must contact his or her user administrator who will reactivate the account. The user administrator will take a different action on the User Administration page to reactivate the account depending on why the account was originally disabled. To reactivate user accounts, the following steps should be followed:

Steps to Reactivate Incorrect Login Lockout

1. Click the **User Administration** link on the left navigation.
2. On the Create New User page, select the option to **Reset User Password**.
3. Click the **Save** button.

   MSIX will generate an email to the user with a temporary password. The user will be prompted to change the temporary password when he/she first logs into MSIX.

Steps to Reactivate Expired Accounts

1. Click the **User Administration** link on the left navigation.
2. On the Create New User page, Change the **Account Expiration** date to a future date and set the **Account Status** to **Enabled**.
3. Click the **Save** button.

Steps to Reactivate Inactive and Manually Disabled Accounts

1. Click the **User Administration** link on the left navigation.
2. On the Create New User page, set the **Account Status** to **Enabled**.

3. Click the **Save** button.

Account Deactivation

User accounts can be deactivated by User Administrators. This is a **permanent change**. A User Administrator cannot later reactivate a deactivated account.

If a user will be leaving his/her organization, he/she should contact his/her user administrator prior to departure date. A user administrator must deactivate a user's account within 24 hours of the user's departure. Once deactivated, the user account cannot be reactivated or reused. Note, the Help Desk does not reset passwords, create new users, deactivate, or disable existing users.

Steps to Deactivate an Account

1. Click the **User Administration** link on the left navigation.
2. On the Create New User page, select the option to **Deactivate Account**.
3. Click the **Save** button.

MSIX will navigate to a Confirmation page where the user administrator will be asked to confirm that he/she wants to permanently deactivate the user account. Once the user administrator confirms the user's action, the account is immediately deactivated.

User Administration Reports

MSIX provides User Administrators with three User Management Reports to view information about the MSIX users in your state. There are three reports found under the Reports link on the Left-side Navigation on the User Administration home page. By clicking on that link, you will reach the "User Management Reports" page that lists the User Account List Report, the User Detail Report, and the User Role Report.

Data contained in the MSIX User Management Reports is retrieved from MSIX periodically throughout the day. Due to these periodic updates, the information contained in the reports may not contain updates made in MSIX within the past hour. You can view a report or print it as you would any web page.

- **User Account List Report** — This report supports "Security Compliance Reviews" to determine if users have the appropriate level of access to MSIX. Reviews are also done to monitor whether a user is still actively using MSIX or if the account should be deactivated.
- **User Detail Report** — This report provides greater detail about users by including location and contact information, which may be helpful if you need to communicate with a group of users.
- **User Role Report** — This report provides users grouped by role, which may be useful to identify individuals for role-based training or if you wanted to add a second role to a user group.

The table below gives a snapshot of the data fields or column headings found in each report.

User Management Reports			
Column Headings	**User Account List**	**User Detail**	**User Role**
Name	✓	✓	✓
User ID	✓	✓	✓
Role		✓	✓

User Management Reports			
Column Headings	User Account List	User Detail	User Role
Status	✓	✓	✓
Address		✓	
Contact *(email & phone #)*		✓	
Organization		✓	✓
Last Login Date	✓		
Account Expiration Date	✓		
Account Activation Date	✓		
Account Creation Date	✓		
Status Date	✓		

Appendix A – Rules of Behavior

Appendix A provides the Rules of Behavior (ROB) that users must review and accept in order to successfully login into MSIX. A link to the ROB is also located within MSIX at the bottom of every screen, and MSIX will also display the ROB to users upon their initial login to MSIX.

Responsibilities

The Migrant Student Information Exchange (MSIX) is a Department of Education (ED) information system and is to be used for official use only. Users must read, understand, and comply with these Rules of Behavior. Failure to comply with the MSIX Rules of Behavior may result in revocation of your MSIX account privileges, job action, or criminal prosecution.

MSIX users must complete a basic security awareness training course prior to being granted access to the system. The security topics addressed in this document provide the required security awareness content, so it is important that you read through this entire text. Users must also complete annual security awareness refresher training. MSIX will prompt you to reread the Rules of Behavior annually (or more often due to changes in the system or regulations) to meet this requirement.

Monitoring

This is a Department of Education computer system. System usage may be monitored, recorded, and subject to audit by authorized personnel. THERE IS NO RIGHT OF PRIVACY IN THIS SYSTEM. Unauthorized use of this system is prohibited and subject to criminal and civil penalties.

System personnel may provide to law enforcement officials any potential evidence of crime found on Department of Education computer systems. USE OF THIS SYSTEM BY ANY USER, AUTHORIZED OR UNAUTHORIZED, CONSTITUTES CONSENT TO THIS MONITORING, RECORDING, and AUDIT.

MSIX Security Controls

MSIX security controls have been implemented to protect the information processed and stored within the system. MSIX users are an integral part in ensuring the MSIX security controls provide the intended level of protection. It is important to understand these security controls, especially those with which you directly interface. The sections below provide detail on some of those controls and the expectations for MSIX users.

MSIX security controls are designed to:

- Ensure only authorized users have access to the system;
- Ensure users are uniquely identified when using the system;
- Tie actions taken within the system to a specific user;
- Ensure users only have access to perform the actions required by their position;
- Ensure MSIX information is not inappropriately released; and
- Ensure MSIX is available to users when needed.

Examples of security controls deployed within MSIX include:

- **Automated Session Timeout** — Users are automatically logged out of MSIX after thirty minutes of inactivity. This helps ensure unauthorized users do not gain access to the system.
- **Role-based Access Control** — User ids are assigned a specific role within MSIX. This role corresponds to the user's job function and restricts access to certain MSIX capabilities.
- **Audit Logging** — Actions taken within MSIX are captured in log files to help identify unauthorized access and enforce accountability within the system.
- **Incident Response** — If a user suspects their user id has been subject to unauthorized use, contact the MSIX help desk immediately.
- **Communication Protection** — Traffic between a user's web browser and the MSIX servers is encrypted to protect it during transmission.

The sections below describe several other security controls in place within MSIX. It is important that you understand and comply with these controls to ensure the MSIX security is maintained.

User Credentials

User credentials are the mechanism by which MSIX identifies and verifies users. These are your user id and password. User ids uniquely identify each MSIX user and allow the MSIX System Administrators to attribute actions taken within the system to a specific user. This tracking is important in enforcing accountability within the system. Passwords are used by MSIX to verify a user's identity. It is important for you to comply with the following rules governing user credentials:

- Protect your logon credentials at all times.
- Never share your user id and/or password with anyone else. You are responsible for all actions taken with your user credentials.
- Your passwords must:
  - Be changed upon initial login to MSIX;
  - Contain at least eight (8) characters;
  - Contain a mix of letters (upper and lower case), numbers, and special characters (#, @, etc.);
  - Be changed at least every ninety (90) days; and
  - Not reuse your previous six (6) passwords.
  - Not match or resemble the word "password" in any form (e.g., as-is, capitalized, or adding a number, etc.);
  - Not contain the same string as the user ID or that contains the user's name; and
  - Not be a dictionary word in any language.
- Do not write your password down or keep it in an area where it can be easily discovered.
- Avoid using the "remember password" feature.
- User accounts are disabled after three (3) consecutive invalid attempts are made to supply a password.
- Reinstatement of a disabled user account can only be reinstated by a Help Desk technician or a system administrator.

Protection of MSIX Information

You are required to protect MSIX information in any form. This includes information contained on printed reports, data downloaded onto computers and computer media (e.g. diskettes, tapes, compact discs, thumb drives, etc.), or any other format. In order to ensure protection of MSIX information, you should observe the following rules:

- Log out of MSIX if you are going to be away from your computer for longer than fifteen minutes.
- Log out of MSIX or lock your computer before you leave it unattended by using the key sequence when leaving your seat.
- Media (including reports) containing MSIX information should be removed from your desktops during non-business hours.
- Store media containing MSIX information in a locked container (e.g. desk drawer) during non-business hours.
- Store digital information in an encrypted format where technically possible.
- Media containing MSIX information should be properly cleansed or destroyed.
  - Shred paper media and compact discs prior to disposal.
  - Diskettes and other magnetic media should be cleansed using appropriate software or a magnetic field with sufficient strength so as to make the information unreadable.
    - Note that simply deleting files from magnetic media does not remove the information from the media.
    - Media containing encrypted information can be excluded from the cleansing process, although it is recommended.
- If the access which you have been granted within MSIX is more than required to fulfill your job duties, it should be reported to appropriate personnel.
- Do not disclose MSIX information to any individual without a "need-to-know" for the information in the course of their business.

Other Security Considerations

This section describes some additional security items of which you should be aware.

- **Incident Response** — If you suspect or detect a security violation in MSIX, contact the MSIX Help Desk immediately. For example, if you suspect someone may have used your user id to log in to MSIX, you should contact the MSIX Help Desk. Other warning signs that MSIX may have been compromised include, but are not limited to: inappropriate images or text on the web pages, data formats that are not what is expected, missing data, or MSIX is not available. While these may not be attributed to a compromise, it is better to have it checked out and be sure than to take no action.
- **Shoulder Surfing** — Shoulder surfing is using direct observation techniques, such as looking over someone's shoulder, to get information. An example of shoulder surfing is when a person looks over someone else's shoulder while they are entering a password for a system to covertly acquire that password. To protect against this type of attack, slouch over your keyboard slightly when keying in your password to block the view of a possible onlooker.
- **Social Engineering** — Social engineering is a collection of techniques used to manipulate people into performing actions or divulging confidential information. For example, a typical social engineering attack scenario is a hacker posing as an authorized user calling a system help desk posing as that user. The hacker, through trickery, coercion, or simply being nice coaxes the help desk technician into providing the login credentials for the user

he is claiming to be. The hacker then gains unauthorized access to the system using an authorized user's credentials.

- The example above is one example of a social engineering technique. Another is when a hacker calls a user at random and pretends to be a help desk technician. Under the guise of purportedly fixing a problem, the hacker requests the user's login credentials. If provided, the user has unwittingly provided system access to an unauthorized person.
- To defeat social engineering simply question anything that doesn't make sense to you. For example, a help desk technician should never ask a user for their login credentials to resolve a problem. If you receive a call from someone and you are not sure who they are, ask for a callback number. Hang up the phone and call back to the number provided. Hackers will typically provide a bogus number. Ask questions. If the answers you receive do not make sense, end the call and report the incident to your local security organization.
- **Faxing** — When faxing MSIX information, call the recipient of the fax and let them know it is coming. Ask them to go to the fax machine so they can pull it off right away so any sensitive information is not left lying around the office.
- **Virus Scanning** — Scan documents or files downloaded to your computer from the Internet for viruses and other malicious code. Virus scanning software should also be used on email attachments.